BUSINESS ASSOCIATE AGREEMENT

This **Business Associate Agreement** ("Agreement") is entered into between Valley Medical Transportation, Inc. ("CLIENT") and SyMed Corporation ("SyMed") and is effective as set forth in Section 6 (a) below.

RECITALS

Business Associate provides certain billing and collection services to CLIENT pursuant to a written Revenue Cycle Management Agreement ("Service Agreement.")

Under the Service Agreement, CLIENT discloses certain information ("Information") to SyMed so that SyMed can perform on CLIENT's behalf certain functions or activities relating to treatment, payment and / or health care operations of CLIENT, some of which information constitutes Protected Health Information ("PHI") as defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA").

The purpose of this Agreement is to satisfy certain standards and requirements of HIPAA and the HIPAA Regulations, including, but not limited to, Title 45, Section 164.504(e) of the Code of Federal Regulations ("CFR"), as the same may be amended from time to time.

In consideration of the mutual promises below and the exchange of information pursuant to this Agreement, the parties agree as follows:

Definitions. Unless otherwise defined in this Agreement, capitalized terms have the meanings ascribed to them under HIPAA, the HIPAA Privacy Rule and Security Standards, as amended by the HITECH Act:

(a) *Billing Company.* "Billing Company" shall mean SyMed Corporation, functioning as a Business Associate of CLIENT pursuant to the Service Agreement as such term is defined under the HIPAA Regulations, including, but not limited to 45 CFR Section 160.103.

(b) *Breach.* "Breach" means the unauthorized acquisition, access, use, or disclosure of Protected Health Information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. The term "Breach" does not include acquisition, access, or use made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual with SyMed if such information is not further acquired, accessed, used, or disclosed by any person; or any inadvertent disclosure from an individual who is otherwise authorized to access Protected Health Information at a facility operated by SyMed to another similarly situated individual at same facility if such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person or other circumstances specified in Regulations or Guidance issued by the Secretary.

(c) *Data Aggregation Services*. Date Aggregation Services means the combining by SyMed of the Protected Health Information of CLIENT with Protected Health Information received by SyMed in its capacity as a SyMed of another CLIENT to permit data analyses that relate to the health care operations of CLIENT or other Covered Entities.

(d) *Medical Practice.* "Medical Practice" shall mean CLIENT, functioning as a Covered Entity under HIPAA as described in the Service Agreement and as such term under HIPAA and the HIPAA Regulations, including, but not limited to, 45 CFR Section 160.103.

(e) *Designated Record Set.* "Designated Record Set" shall mean a group of records maintained by or for CLIENT that are (i) the medical records and billing records about individuals maintained by or for CLIENT; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for CLIENT to make decisions about individuals. For purposes of this definition, record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for CLIENT.

(f) *Guidance.* "Guidance" shall mean official guidance of the Secretary as specified in the HITECH Act and any other official guidance or interpretation of HIPAA by a federal governmental agency with jurisdiction.

(g) *HITECH Act.* "HITECH Act" shall mean the Health Information Technology for Economic and Clinical Health Act, enacted as Title XIII, Subtitle D of the American Recovery and Reinvestment Act or 2009, and implementing Regulations and Guidance.

(h) *Individual*. "Individual" shall have the same meaning as the term "individual" in 45 CRF 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

(i) *Privacy Rule*. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E, as amended by the HITECH Act.

(j) *Protected Health Information or PHI and ePHI* "Protected Health Information" and "PHI" shall have the same meaning as the term "protected health information" in 45 CFR 164.501. References to PHI shall be deemed to include references to PHI in electronic form held by SyMed ("ePHI") unless stated otherwise. SyMed's obligations under this Agreement apply only to Protected Health Information created or received by SyMed from or on behalf of CLIENT, and the term Protected Health Information refers only to Protected Health Information created or received by SyMed from or on behalf of CLIENT under the Service Agreement.

(k) *Required By Law.* "Required By Law" means a mandate contained in law that compels SyMed or CLIENT to make a use or disclosure of Protected Health Information and that is enforceable in a court of law. Required by Law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

(l) *Security Incident.* "Security Incident" means a successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

(m) *Security Standards.* "Security Standards" shall mean the Security Standards at 45 CFR parts 160, 162 and 164, as may be amended or supplemented during the term of this Agreement and all applicable Guidance.

(n) *Service Agreement*. "Service Agreement" shall mean the agreement or agreements between CLIENT and SyMed under which SyMed performs third party billing or other specified functions or activities on behalf of CLIENT which involve the PHI of CLIENT. In the event there are multiple Service Agreements, this Agreement shall be interpreted as applying separately to each.

(o) *Secretary*. "Secretary" shall mean the Secretary of the Department of Health and Human Services or her designee.

(p) "*Unsecured Protected Health Information*" Unsecured Protected Health Information means Protected Health Information that is not secured through the use of a technology or methodology specified by the Secretary in published Regulations or Guidance.

2. Obligations and Activities of SyMed as to Protected Health Information.

SyMed agrees to not use or further disclose Protected Health Information other than as permitted or required by the Service Agreement, this Agreement or as required by law.

SyMed agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by the Service Agreement and /or this Agreement. As to ePHI, SyMed will comply with the applicable provisions of the Security Standards, by providing Administrative, Physical, and Technical Safeguards for all ePHI and by developing Policies and Procedures implementing those Safeguards.

(a) (1) SyMed agrees to report to CLIENT any use or disclosure of the Protected Health Information not provided for by the Service Agreement and/or this Agreement. Without limiting the foregoing, SyMed agrees to report to CLIENT any Breach of Protected Health Information accessed, maintained, retained, modified, stored, destroyed or otherwise held or used in unsecured form by SyMed. SyMed will provide written notice of any such Breach to CLIENT in the manner and to the recipient designated in the Service Agreement, unless the parties agree in writing in advance on another method or recipient of such notice, within seven (7) business days of the first day the Breach is known, or reasonably should have been known,

to SyMed, including for this purpose known to any employee, officer, or other agent of SyMed (other than the individual committing the Breach) ("Breach Notice"). The Breach Notice will include the identification of each individual whose Unsecured Protected Health Information was subject to the Breach, the nature of the PHI that was subject to the Breach and the circumstances of the Breach, to the extent known to SyMed as of the date of the Breach Notice. SyMed will take reasonable steps to mitigate the effects on the Breach, coordinating such efforts with CLIENT. SyMed will diligently pursue investigation of the Breach and notify CLIENT in writing as soon as reasonably possible, but in no event later than thirty (30) business days after the date of the Breach Notice of the names of all individuals whose Unsecured PHI was subject to the Breach, of the full circumstances of the Breach and of any other information related to the Breach SyMed discovers, all to the extent available to SyMed after using all reasonable efforts to investigate. SyMed will promptly provide other information relating to the Breach as reasonably requested by CLIENT and available to SyMed.

(2) Notice to individuals or governmental agencies will be provided solely by CLIENT no later than sixty (60) days after discovery of the Breach, in a form determined by CLIENT, provided however, the notice shall include a brief description of how the Breach occurred, the date of the Breach and the date of the discovery of the Breach, if known, a description of the types of unsecured PHI that were involved in the Breach, any steps individuals should take to protect themselves from potential harm resulting from the Breach; a brief description of what is being done to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches; and contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address; and provided that (i) CLIENT will discuss, in advance of any decision by CLIENT as to providing notice to individuals, the Secretary or other agencies, any harm threshold analysis (whether under the HITECH Act or under applicable Regulations or Guidance) made by the CLIENT as to the Breach and (ii) be given a copy of any proposed notice and a list of its intended recipients, in both cases at least three (3) days in advance. During that time period SyMed may provide comments to CLIENT as to accuracy and completeness of the harm threshold analysis or the statements contained in the notice, which comments shall be reasonably considered by CLIENT. Unless specifically provided otherwise in the Service Agreement, CLIENT will be deemed an independent contractor, and not an agent, of SYMED for purposes of Breach Notification. In the event that the Breach also implicates a state law requiring notification of individuals or agencies, SYMED will have the same rights as to the notice to be given by CLIENT specified above.

(3) In the event that CLIENT experiences a Breach, other than a Breach solely and directly attributable to and by SyMed, and requests SyMed's assistance in analyzing or responding to the Breach, SyMed will use reasonable efforts to comply, provided that SyMed may charge CLIENT reasonable amounts for time and materials provided, which shall be negotiated prior to commencement of work and will be paid promptly by CLIENT upon receipt of a statement therefor and provided further that CLIENT is solely responsible for all aspects of the content, timing and provision of notice to individuals and agencies.

SyMed agrees to mitigate, to the extent practicable, any harmful effect that is known to SyMed of a use or disclosure of Protected Health Information by SyMed in violation of the requirements of the Service Agreement and / or this Agreement.

SyMed agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by SyMed on behalf of CLIENT agrees to the same restrictions and conditions that apply through this Agreement to SyMed with respect to such information.

To the extent SyMed maintains an original Designated Record Set an behalf of CLIENT, SyMed agrees to provide access, at the request of CLIENT, and in the time and manner designated by CLIENT, to Protected Health Information in a Designated Record Set, to CLIENT in order to meet the requirements under 45 CFR 164.524.

SyMed agrees to make any amendment(s) to Protected Health Information in a Designated Record Set maintained by SyMed that CLIENT directs or agrees to pursuant to 45 CFR 164.526, at the request of CLIENT, and in the time and manner designated by CLIENT and as required under 45 CFR 164.526.

SyMed agrees to make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by SyMed on behalf of CLIENT available at the request of CLIENT to the Secretary, in a time and manner designated by the Secretary, for purposes of the Secretary determining CLIENT's compliance with the Privacy Rule.

SyMed agrees to document such disclosures of Protected Health Information and information related to such disclosures as would be required for CLIENT to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528. If CLIENT uses or maintains an Electronic Health Record(s), as defined in the HITECH Act, CLIENT will advise SyMed of that fact and SyMed and CLIENT will meet and discuss whether SyMed's accounting obligations are required under the HITECH Act to include disclosures by SyMed for purposes of Treatment, Payment and Health Care Operations ("TPO Accounting"); provided that: (i) CLIENT will provide such notice to SyMed at least fifteen

(15) in advance of the effective date of disclosures that SyMed is obligated to report disclosures for a TPO Accounting under this paragraph; and (ii) SyMed may make a reasonable additional charge, on an accounting-by-accounting basis or through an upward adjustment to its fees or cost pass-throughs under the Service Agreement, reasonably calculated to cover SyMed's additional costs to provide such a TPO accounting. TPO Accounting shall be provided in accordance with Regulations promulgated by the Secretary. Unless the parties agree otherwise, in writing, in the event of an individual's request for an accounting, Business Associate will provide information it is required to maintain pursuant to this Agreement to CLIENT and CLIENT will provide the accounting to the individual.

Upon reasonable advance notice, SyMed will provide individuals with access to their Protected Health Information in an electronic format and transmit such information in electronic format directly to an entity specified by the individual, to the extent the individual's PHI is CLIENT's PHI held or controlled by SyMed, in accordance with the HITECH Act amendments to the Privacy Rule. SyMed may make a reasonable charge to CLIENT or to, to the extent permitted by the HITECH Act, Regulations, or Guidance, the individual for such transmission.

SyMed will not, directly or indirectly, exchange CLIENT's PHI or CLIENT's Electronic Health Records for direct or indirect remuneration unless specifically provided for in the Service Agreement. In this regard, SyMed will comply with all applicable Regulations published by the Secretary.

3. Permitted Uses and Disclosures of Protected Health Information by SyMed. ***Except as otherwise limited in the Service Agreement and/or this Agreement, SyMed may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of,*** CLIENT ***as specified in the Service Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by*** CLIENT**, *including the following:***

Except as otherwise limited in this Agreement, SyMed may disclose Protected Health Information for the proper management and administration of SyMed or to carry out legal responsibilities of SyMed, provided that disclosures are required by law, or SyMed obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies SyMed of any instances of which it is aware in which the confidentiality of the information has been breached.

SyMed may use Protected Health Information to provide Data Aggregation services to CLIENT as permitted by 45 CFR 164.504(e)(2)(i)(B) to the extent required under the Service Agreement.

SyMed may use Protected Health Information to create information that is not individually identifiable health information, as permitted by 45 CFR 164.502(d) and 164.514 ("De-identified Information"). SyMed shall own the De-identified Information, under copyright and all other applicable laws or legal doctrines.

4. Obligations of CLIENT to Inform SyMed of Privacy Practices and Individual Restrictions.

CLIENT shall provide SyMed with the notice of privacy practices that CLIENT produces in accordance with 45 CFR 164.520, as well as any changes to such notice.

CLIENT shall notify SyMed of any restriction on the use or disclosure of Protected Health Information that CLIENT has agreed to in accordance with the Privacy Rule in excess of the restrictions required by that rule, to the extent that such restriction may affect SyMed's use or disclosure of Protected Health Information, at least seven (7) in advance of the date upon which compliance by SyMed is required. If CLIENT agrees not to disclose an item or service paid for entirely out-of-pocket by an individual to a Health Plan for payment or health care operations purposes, unless such disclosure is required by law ("Self-Pay Services"), the following additional conditions shall apply: (i) CLIENT is solely responsible for determining whether there is an applicable legal requirement that requires such disclosure; (b) SyMed may rely on CLIENT's instructions not to disclose; and (iii) CLIENT will indemnify and hold SyMed harmless from costs or damages arising from such reliance. SyMed may make a reasonable charge on an instance-by-instance, or such other basis that the parties may agree, for compliance with CLIENT's instructions and CLIENT will pay such charges promptly upon receipt of an invoice or statement. SyMed will use all reasonable efforts comply with all such limitations subject to timely receipt of notice from CLIENT as specified above.

5. Permissible Requests or Disclosures

Except as specifically provided in the Service Agreement or in this Agreement, CLIENT shall not request SyMed to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by CLIENT.

Without limiting the generality of the foregoing, under the Service Agreement, CLIENT will provide, and SyMed will request, no more than the minimum necessary amount of PHI required for the performance of SyMed's services under the Service Agreement. SyMed and CLIENT will comply with the Guidance on minimum necessary to be issued by the Secretary as to the Minimum Necessary as reasonably requested by CLIENT.

6. Term and Termination

(a) *Term*. This Agreement is effective as of January 16, 2014 and replaces any prior Business Associate Agreement between the parties relating to the Service Agreement. This Agreement shall terminate when the Service Agreement terminates and all of the Protected Health Information provided by CLIENT to SyMed, or created or received by SyMed on behalf of CLIENT, is destroyed or returned to CLIENT, or if it is not feasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions of subparagraph (c) of this Section 6.

(b) *Termination for Cause.*

Upon CLIENT's knowledge of a material breach by SyMed, CLIENT shall provide an opportunity for SyMed to cure the breach or end the violation and CLIENT may terminate the Service Agreement if SyMed does not cure the breach or end the violation within the time specified by CLIENT, which shall not be less than three (3) days;

Notwithstanding the foregoing Section (b) (1), CLIENT may immediately terminate the Service Agreement if SyMed has breached a material term of this Agreement and CLIENT determines that cure is not possible.

Notwithstanding the foregoing Section (b) (1) or (2), if CLIENT determines that neither cure, as specified in Section (b) (1) above nor termination, as specified in Section (b) (2) above, is feasible, CLIENT shall report the violation to the Secretary.

In the event that SyMed becomes aware of a pattern of activity or a practice of CLIENT that constitutes a material violation of the obligations of CLIENT under this Agreement, SyMed will have the same rights and obligations specified as to CLIENT in Sections 6 (b) (1), (2) and (3).

(c) *Effect of Termination.*

Except as provided in paragraph (b) of this section, upon termination of the Service Agreement for any reason, SyMed shall return or destroy all Protected Health Information received from CLIENT or created or received by SyMed on behalf of CLIENT. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of SyMed. SyMed shall retain no copies of the Protected Health Information.

In the event that SyMed determines that returning or destroying the Protected Health Information is not feasible, SyMed shall provide to CLIENT notification of the conditions that make return or destruction impossible. SyMed shall thereafter extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction impossible, for so long as SyMed maintains such Protected Health Information.

7. Miscellaneous

(a) *Regulatory References*. A reference in this Agreement to a section in the Privacy Rule, the Security Standards, or Regulations or Guidance means the referenced material as in effect as of the Effective Date or as subsequently amended or as supplemented or implemented.

(b) *Amendment*. The parties agree that in the event that either party reasonably determines that the provisions of this Agreement or of the Service Agreement require amendment based on the HITECH Act (including but not limited to Guidance or Regulations to be published by the Secretary after the Effective Date of this Agreement) or other legislative or regulatory changes to the Privacy Rule or the Security Standards, the party may notify the other in writing, including the basis for its belief in reasonable detail, and the parties will thereafter promptly meet and negotiate appropriate amendments to this Agreement necessary to assure compliance by either or both SyMed or CLIENT. If the parties are unable to agree on such changes, in writing, within thirty (30) of receipt of the notice, either party may terminate the Service Agreement, without cost or penalty unless otherwise specifically provided for in the Service Agreement, upon the earlier of (i) the date

on which the proposed amendment was required by law or Regulation to be effective or (ii) sixty (60) days advance written notice.

(c) *Survival*. The respective rights and obligations of the parties under this Agreement which require or contemplate compliance after termination of this Agreement shall survive the termination.

(d) *Interpretation*. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits both CLIENT and SyMed to comply with the Privacy Rule or the Security Standards, as appropriate, consistent with the Service Agreement.

In witness whereof, CLIENT and SyMed have executed this Business Associate Agreement effective as set forth above.

Valley Medical Transportation	SyMed Corporation
By: _____	By: _____
Title: _____	Title: _____